

CLAIMS

What is claimed is:

- 1 1. A digital camera comprising:
2 a memory to store image data of a captured image representing a scene
3 in the physical world; and
4 an encryption module configured to digitally sign the image data prior to
5 storage using a private key of an asymmetric key pair.
6
- 1 2. The digital camera of claim 1, wherein the encryption module is
2 configured to obtain metadata associated with the image data and to digitally
3 sign the image data and the metadata.
4
- 1 3. The digital camera of claim 1, wherein the metadata comprises at least
2 one of date and time the image was captured, at least one of name and identifier
3 of the camera owner, at least one of name and identifier of the photographer,
4 focal distance, white levels, f-stop, brightness compensation, and distance for
5 auto-focus, and digital signature of the image data, when the image was
6 captured.
7
- 1 4. The digital camera of claim 1, further comprising a global positioning
2 system (GPS) detector configured to determine a geographic location of the
3 digital camera and wherein the metadata comprises the geographic location of
4 the camera when the image was captured.
5
- 1 5. The digital camera of claim 1, wherein the private key is uniquely
2 associated with the digital camera.
3
- 1 6. The digital camera of claim 1, wherein the private key is uniquely
2 associated with a manufacturer of the digital camera.

3
1 7. The digital camera of claim 1, wherein the private key is uniquely
2 associated with an owner of the digital camera.
3

1 8. The digital camera of claim 1, wherein the encryption module is
2 tamper-resistant.
3

1 9. A digital photography subsystem comprising:
2 a decryption module to accept image data and metadata from a digital
3 camera, the metadata including a digital signature of the image data, and to
4 verify the digital signature of the image data to determine authenticity of an
5 image represented by the image data; and
6 a viewer module to display the image data when the decryption module
7 indicates the image data is authentic.
8

1 10. The digital photography subsystem of claim 9, wherein the decryption
2 module is further configured to examine the metadata to determine authenticity
3 of the image data.
4

1 11. The digital photography subsystem of claim 10, wherein the metadata
2 comprises at least one of date and time the image was captured, at least one of
3 name and identifier of the camera owner, at least one of name and identifier of
4 the photographer, focal distance, white levels, f-stop, brightness compensation,
5 and distance for auto-focus, when the image was captured.
6

1 12. The digital photography subsystem of claim 11, wherein the metadata
2 comprises a geographic location of the digital camera when the image was
3 captured and the decryption module is configured to examine the geographic
4 location when determining authenticity of the image.
5

1 13. The digital photography subsystem of claim 11, wherein the viewer
2 module is configured to display the metadata in addition to the image data.
3

1 14. The digital photography subsystem of claim 11, wherein the image
2 data and metadata is associated with audit data indicating changes to the image
3 data, and the viewer module is configured to display the audit data.
4

1 15. A secure digital photography system comprising:
2 a digital camera including a memory to store image data of a captured
3 image representing a scene in the physical world, and an encryption module
4 configured to digitally sign the image data prior to storage using a private key of
5 an asymmetric key pair and to obtain metadata associated with the image data,
6 the metadata including the digital signature of the image data; and
7 a digital photography subsystem including a decryption module to accept
8 image data and metadata from the digital camera and to verify the digital
9 signature of the image data to determine authenticity of the captured image
10 represented by the image data using a public key of the asymmetric key pair,
11 and a viewer module to display the image data when the decryption module
12 indicates the image data is authentic.
13

1 16. The secure digital photography system of claim 15, wherein the
2 metadata comprises at least one of: date and time the image was captured, at
3 least one of name and identifier of the camera owner, at least one of name and
4 identifier of the photographer, focal distance, white levels, f-stop, brightness
5 compensation, and distance for auto-focus, and digital signature of the image
6 data, when the image was captured.
7

1 17. The secure digital photography system of claim 16, wherein the digital
2 camera further comprises a global positioning system (GPS) detector configured
3 to determine geographic location of the digital camera and wherein the metadata
4 comprises the geographic location of the camera when the image was captured.

5
1 18. The secure digital photography system of claim 16, wherein the
2 decryption module is further configured to examine the metadata to determine
3 authenticity of the image data.

4
1 19. A method of generating photograph data comprising:
2 capturing image data representing an image in the physical world by a
3 digital camera;
4 obtaining metadata associated with the captured image;
5 digitally signing the image data with a private key of an asymmetric key
6 pair; and
7 storing the image data and metadata in a memory of the digital camera.

8
1 20. The method of claim 19, wherein the metadata comprises at least
2 one of date and time the image was captured, at least one of name and identifier
3 of the camera owner, at least one of name and identifier of the photographer,
4 focal distance, white levels, f-stop, brightness compensation, and distance for
5 auto-focus, and digital signature of the image data, when the image was
6 captured.

7
1 21. The method of claim 20, further comprising digitally signing the
2 metadata prior to storage.

3
1 22. The method of claim 20, further comprising determining a geographic
2 location of the digital camera and wherein the metadata comprises the
3 geographic location of the camera when the image was captured.

4
1 23. The method of claim 19, wherein the private key is uniquely
2 associated with the digital camera.

1 24. The method of claim 19, wherein the private key is uniquely
2 associated with a manufacturer of the digital camera.
3

1 25. The method of claim 19, wherein the private key is uniquely
2 associated with an owner of the digital camera.
3

1 26. A method of generating and authenticating digital photographs
2 comprising:
3 capturing image data representing an image in the physical world by a
4 digital camera;
5 obtaining metadata associated with the captured image, the metadata
6 indicating characteristics of the image data;
7 digitally signing the image data with a private key of an asymmetric key
8 pair; and
9 transferring the image data, the digital signature, and the metadata to a
10 host system;
11 authenticating the image data by the host system using the digital
12 signature, a corresponding public key of the asymmetric key pair, and the
13 metadata.
14

1 27. The method of claim 26, wherein the metadata comprises at least
2 one of date and time the image was captured by the digital camera, at least one
3 of name and identifier of the camera owner, at least one of name and identifier of
4 the photographer, focal distance, white levels, f-stop, brightness compensation,
5 and distance for auto-focus, when the image was captured.
6

1 28. The method of claim 27, further comprising obtaining the date and
2 time setting for the digital camera by the host system from a website controlled
3 by at least one of the manufacturer and the distributor of the digital camera.
4

1 29. The method of claim 26, further comprising updating the private key
2 for the digital camera by the host system from a website controlled by at least
3 one of the manufacturer and the distributor of the digital camera.
4

1 30. The method of claim 27, further comprising determining a geographic
2 location of the digital camera when capturing the image and wherein the
3 metadata comprises the geographic location of the camera when the image was
4 captured.
5

1 31. The method of claim 26, further comprising displaying the image data
2 when authenticated.
3

1 32. The method of claim 26, further comprising updating audit data
2 describing changes made to the image data, and associating the audit data with
3 the image data and the metadata.